

Projekts uz 03.03.2023.

Vēlamais izskatīšanas laiks:

Finanšu komitejā 15.03.2023.

domē 22.03.2023.

Ziņotājs: M.Lazdiņš

APSTIPRINĀTI

Ādažu novada pašvaldības domes sēdē

2023. gada 22. martā (protokols Nr. \_\_ § \_\_)

NOTEIKUMI

Ādažos, Ādažu novadā

2023. gada 22. martā  **Nr. X/2023**

**Ādažu novada pašvaldības informācijas sistēmu drošības politika**

*Izdoti saskaņā ar**Informācijas tehnoloģiju drošības likuma 8. pantu un* *Ministru kabineta 28.07.2015. noteikumu Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”*

*13. un 15.punktu*

# Vispārīgie noteikumi

1. Šie noteikumi nosaka pamatprincipus, kādos Ādažu novada pašvaldība (turpmāk – Pārzinis) un tā iestādes un struktūrvienības (turpmāk arī – institūcijas) nodrošina informācijas, informācijas sistēmu un tām saistīto tehnoloģisko resursu drošību, pieejamību, integritāti un konfidencialitāti.
2. Noteikumos lietotie termini:
   1. **par tehniskajiem resursiem atbildīgā persona** – Pārziņa atbildīgā persona, kurai ar amata aprakstu uzticēta atbildība par informācijas tehnoloģiju resursiem un to drošību (Informācijas tehnoloģijuadministrators);
   2. **datu aizsardzības speciālists** – persona, kas uz civiltiesiska līguma pamata pilda datu aizsardzības speciālistam noteiktos uzdevumus institūcijās, un kas sasniedzama, izmantojot pašvaldības oficiālā e-pasta adresi, ar norādi “Datu aizsardzības speciālistam”;
   3. **informācijas sistēma** (turpmāk - IS) – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kas nodrošina Pārziņa funkciju izpildei nepieciešamās informācijas ierosināšanu, radīšanu, apkopošanu, uzkrāšanu, apstrādāšanu, izmantošanu un iznīcināšanu;
   4. **IS tehniskie resursi –** serveri, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas uzglabāšanai un apritei;
   5. **IS informācijas resursi** – datu faili, datu bāzes, arhīvi, u.c. informācija;
   6. **IS lietotājs** **–** persona, kurai darba pienākumu veikšanai piešķirta datortehnika un piekļuves tiesības darbam Pārziņa IS;
   7. **IS ārējie lietotāji** – personas, kurām ir tiesisks pamats un nodrošinātas tehniskas iespējas piekļūt Pārziņa IS;
   8. **drošības incidents** - jebkāds kaitīgs notikums vai nodarījums, kura rezultātā tiek vai var tikt ietekmēta IS integritāte, konfidencialitāte un pieejamība;
   9. **risks** - varbūtība, ka īstenojoties drošības apdraudējumam, Pārziņa informācijas vai tehniskie resursi varētu mainīties, sabojāties, tikt iznīcināti vai nonākt tādu personu rīcībā, kuras nav tam pilnvarotas, vai piekļūšana informācijas resursiem varētu būt traucēta, vai neiespējama;
   10. **integritāte** - nesankcionēta lietotāja veiktās informācijas izmaiņas nav iespējamas (vai vismaz ir atklātas), un autorizēto lietotāju veiktās izmaiņas tiek izsekotas;
   11. **auditācijas pieraksti** – analīzei pieejami pieraksti, kuros reģistrēti dati par konkrētiem IS notikumiem (piekļuve, datu ievade, maiņa, dzēšana, izvade, u.c.).
3. Politika attiecas uz Pārziņa pārvaldībā esošiem informācijas un tehniskajiem resursiem, un ir saistoša visiem Pārziņa darbiniekiem, kuri ir tiesīgi izmantot Pārziņa informācijas un tehniskos resursus (saņem, apstrādā, ievada, pārsūta vai uzglabā informāciju), kā arī tiem ārpakalpojumu sniedzējiem, kuri Pārzinim sniedz ar informācijas tehnoloģijām saistītus pakalpojumus.

# II. IS drošības politikas mērķi un pamatnostādnes

1. IS drošības politikas mērķis ir:
   1. nodrošināt informācijas pieejamību;
   2. nodrošināt informācijas integritāti;
   3. nodrošināt informācijas konfidencialitāti;
   4. aizsargāt IS informācijas resursus;
   5. aizsargāt IS tehniskos resursus;
   6. noteikt IS drošības apdraudējumus;
   7. novērtēt IS drošības riskus;
   8. atklāt IS drošības incidentus;
   9. atjaunot IS darbību pēc drošības incidentiem.
2. Pārzinis nodrošina, ka tā rīcībā esošā informācija tiek apstrādāta, glabāta un  
   pārvaldīta droši un pārbaudāmi, nosakot IS lietotājiem skaidras prasības  
   IS izmantošanā, kā arī organizē IS aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.
3. IS lietotājus iepazīstina ar šiem noteikumiem pirms darba uzsākšanas institūcijās.
4. Par tehniskajiem resursiem atbildīgā persona kontrolē šo un citu pakārtoto noteikumu ievērošanu:
   1. Informācijas sistēmas lietošanas noteikumi;
   2. Informācijas sistēmu atjaunošanas plāns;
   3. Informācijas sistēmu drošības riska pārvaldības plāns;
   4. Informācijas sistēmu drošības iekšējie noteikumi.

**III. IS raksturojums un analīze drošības jomā**

1. Visiem Pārziņa IS resursiem (t.sk., darba stacijām, serveriem, perifērijas iekārtām, programmatūrai, IS datiem) jābūt uzskaitītiem un reģistrētiem, kā arī IS datiem ir jābūt klasificētiem.
2. Par tehniskajiem resursiem atbildīgā persona izvērtē Pārziņa funkciju izpildei izmantoto katru IS, nosakot tai drošības (pieejamības, integritātes un konfidencialitātes) klasi (tabulas veidā) un nodrošina tās uzturēšanu aktuālā versijā (pielikumā):
   1. ja IS neplānots pārtraukums paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī, tai piešķir C pieejamības klasi;
   2. ja IS neplānots pārtraukums paredzētajā darba laikā ir ne lielāks par 24 stundām mēnesī, un ir pieļaujams vairāk par 4 stundām mēnesī, tai piešķir B pieejamības klasi;
   3. ja IS neplānots pārtraukums paredzētajā darba laikā ir ne lielāks par 4 stundām mēnesī, tai piešķir A pieejamības klasi;
   4. ja IS datu integritātes apdraudējums nerada risku institūcijas pamatfunkciju nodrošināšanai, tai piešķir C integritātes klasi;
   5. ja atsevišķu IS glabāto datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai, tai piešķir B integritātes klasi;
   6. ja IS datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai, tai piešķir A integritātes klasi;
   7. ja IS satur tikai publiski pieejamu informāciju vai tās informācijas neatļauta izpaušana vai noplūde nerada risku pašvaldību institūcijai, tai piešķir C konfidencialitātes klasi;
   8. ja IS tiek apstrādāta ierobežotas pieejamības informācija, izņemot sensitīvus personas datus, vai informācijas neatļauta izpaušana vai noplūdes vienīgās sekas ir iespējamais kaitējums institūcijas reputācijai, tai piešķir B konfidencialitātes klasi;
   9. ja IS tiek apstrādāti sensitīvi personas dati vai informācijas neatļauta izpaušana, vai noplūde var radīt smagākas sekas, nekā kaitējums  institūcijas reputācijai, tai piešķir A konfidencialitātes klasi.
3. Ja IS piešķirtas trīs B klases vai vismaz viena A klase, IS uzskatāma par paaugstinātas drošības sistēmu. Pārējos gadījumos tā uzskatāma par pamata drošības sistēmu.
4. IS drošības klasificēšanai par tehniskajiem resursiem atbildīgā persona var pieaicināt datu aizsardzības speciālistu.

# IV. IS drošības pārvaldības organizācijas principi

1. Pārzinis izstrādā un regulāri uztur un pilnveido dokumentu un pasākumu kopumu, kuru izpilde nodrošina IS drošības politikas mērķu sasniegšanu:
   1. Pārzinis veic darbinieku regulāru izglītošanu, veicinot viņu izpratni par pienākumiem IS risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā;
   2. Pārzinis nodrošina drošības politikas izpildes pastāvīgu pārraudzīšanu;
   3. Pārzinis nosaka IS drošības pienākumu un atbildības skaidru sadalījumu;
   4. Pārzinis nodrošina nepieciešamos līdzekļus un atbalstu IS drošības politikas  
      ieviešanai, uzturēšanai un pilnveidošanai;
   5. atbildīgā persona par IS drošības pārvaldību ir par tehniskajiem resursiem atbildīgā persona, kas:
      1. organizē Pārziņa IT drošības pārvaldību;
      2. organizē IS risku analīzi;
      3. nodrošina nepieciešamo IS drošības dokumentu uzturēšanu un īstenošanu;
      4. reizi gadā veic IT drošības pārbaudi un organizē trūkumu novēršanu;
      5. reizi gadā apmeklē Drošības incidentu novēršanas institūcijas organizētu apmācību IT drošības jautājumos;
      6. atbild par IS tehnisko resursu iegādi, izstrādi, darbību un uzturēšanu;
      7. nodrošina IS tehniskos un loģiskos aizsardzības pasākumus;
      8. atbild par IS pieejas tiesību pārvaldību;
      9. veic IS darbības atjaunošanas pasākumus, ja IS darbība ir traucēta;
      10. atbild par piekļuves kontroli informācijas resursam;
      11. klasificē viņa turējumā esošos informācijas resursus;
      12. nosaka drošības prasības informācijas resursiem;
      13. reizi gadā veic darbinieku instruktāžu IT drošības jautājumos;
   6. IS lietotāji:
      1. iepazīstas un apņemas ievērot informācijas drošības jomā pieņemto iekšējo normatīvo aktu un personu datu aizsardzības prasības;
      2. ne retāk kā reizi gadā iziet darbinieku instruktāžu IT drošības jautājumos.
      3. nekavējoties ziņo par IS identificētajiem riskiem, informācijas drošības notikumiem un incidentiem.

**V. IS drošības atbilstība**

1. Pārzinis veic drošības pasākumu organizēšanu un iekšējo normatīvo aktu izstrādi, precizēšanu un papildināšanu.
2. Pārzinis organizē IS drošības dokumentācijas atbilstības normatīvo aktu prasībām pārskatīšanu.Ja tiek konstatēti būtiski trūkumi, Pārzinis veic pasākumus to novēršanai.
3. Izmaiņas veicamas arī šādos gadījumos:
   1. mainījušies vai ir atklāti jauni IS drošības apdraudējumi;
   2. pieaug IS drošības incidentu skaits vai ir noticis nozīmīgs drošības incidents;
   3. izmaiņas Pārziņa organizatoriskajā struktūrā skar IS drošības vadības organizāciju;
   4. izdarīti grozījumi normatīvajos aktos, kas regulē IS darbību.

# VI. IS drošības principi

1. Risku ierobežošana un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamiem zaudējumiem vai kaitējumu, kas varētu rasties drošības incidenta īstenošanās vai IS darbības pārtraukšanas gadījumos.
2. Komunikāciju un IT darbību pārvaldību realizē, gan izmantojot tehniskus līdzekļus, gan organizatoriskus risinājumus, nodrošinot IS informācijas un tehnisko resursu drošību saskaņā ar funkcionālajām vajadzībām un vadības norādēm.
3. IS tehnisko un informācijas resursu ekspluatāciju realizē, vadoties no resursu ražotāju noteiktām ekspluatācijas normām un iekšējiem normatīvajiem aktiem.
4. IS resursu ekspluatāciju realizē, nodalot izpildes funkcijas no kontroles funkcijām.
5. IS aizsardzību pret destruktīvām programmām un kodiem balsta uz speciālu programmatūru izmantošanu to atklāšanai, neitralizēšanai un iznīcināšanai, kā arī uz lietotāju izglītošanu un nodrošinot IS piekļuves un izmaiņu pārvaldību.
6. Pārziņa valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos IS, tiek iekļautai pretvīrusu funkcionalitāte.
7. Regulāri tiek veidotas un uzglabātas attālinātā vietā informācijas rezerves kopijas.  Informācijas atjaunošanas iespējamība no rezerves kopijām tiek regulāri pārbaudīta.
8. Informācijas apmaiņu ar valsts iestādēm un organizācijām nodrošina saskaņā ar normatīvo aktu prasībām, minimizējot riskus, kas rodas, pārsūtot vai transportējot konfidenciālu informāciju nedrošā vidē.
9. Tiek nodrošināta IS auditācijas pierakstu veidošana un uzglabāšana:
   1. pamata drošības IS - 6 mēnešus pēc ieraksta izdarīšanas;
   2. paaugstinātas drošības IS - 18 mēnešus pēc ieraksta izdarīšanas.
10. Paaugstinātas drošības IS auditācijas pierakstos nodrošina, ka tajos norādītais laiks sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC) ar vienas sekundes precizitāti. Atbildīgā persona nodrošina auditācijas pierakstu plānveida uzraudzību un analīzi.
11. Par tehniskajiem resursiem atbildīgā persona nodrošina, lai jebkura piekļuve IS ir izsekojama līdz konkrētam lietotāja kontam un interneta protokola (IP) adresei.
12. ITN nodrošina, ka Pārziņa pārziņā esošās iekārtas, tai skaitā infrastruktūras iekārtas, kas nodrošina IS funkcionēšanu, neizmanto noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles.
13. Par tehniskajiem resursiem atbildīgā persona nodrošina, ka datu plūsma starp paaugstinātas drošības IS un tās lietotājiem, kā arī starp paaugstinātas drošības IS un citām IS tiek kontrolēta.
14. IS lietotāji, kam piešķirtas IS administrēšanas tiesības, izmanto īpašus lietotāju kontus (turpmāk – Sistēmas administratora konti), kas netiek izmantoti ikdienas darbību veikšanai.
15. Katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja IS ir lietotāja konts, kas nav piesaistāms konkrētai fiziskai personai, piemēram, starpsistēmu tehnoloģiskais konts, tad IS tiek iestrādāti tehniski līdzekļi, kas novērš iespēju lietotājiem izmantot šos kontus.
16. Par tehniskajiem resursiem atbildīgā persona izmanto kriptogrāfiskas kontroles lietotāju autentificēšanai, kā arī, lai nodrošinātu informācijas konfidencialitāti, integritāti un lietotāju veikto darbību nenoliegšanu.
17. Lietotāja tiesību piešķiršana, anulēšana, un IS lietošanas un aizsardzības noteikumi noteikti Pārziņa normatīvajā aktā “Informācijas sistēmu lietošanas noteikumi”, ar ko katru IS lietotāju iepazīstina elektroniski DVS pirms IS lietošanas tiesību piešķiršanas.
18. Katram IS lietotājam jāizveido parole, kuras garums ir vismaz 9 simboli un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un speciālu simbolu.
19. IS nav pieļaujama funkcionalitāte, kas atļauj IS lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada.
20. IS lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas. Tā nekavējoties jānomaina.
21. IS lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros, izņemot 36. punktā gadījumā.
22. IS lietotāja parole ievadīšanas brīdī netiek pilnībā attēlota lietotājam.
23. Parole obligāti jāmaina ne vēlāk kā pēc 90 dienām, to aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā. IS lietotāja parole nedrīkst sakrist ne ar vienu no 5 iepriekšējām IS lietotāja parolēm. Piecas secīgas reizes nepareizi ievadot IS lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts.
24. Sistēmkontus aizsargā tā, lai novērstu iespēju lietotājiem tos izmantot.
25. Par tehniskajiem resursiem atbildīgā persona veic pieejamo programmatūras atjauninājumu izvērtēšanu un nepieciešamības gadījumā – testēšanu.
26. IS tiek nodrošināti visi pieejamie un nepieciešamie programmatūras atjauninājumi.
27. Pirms IS resursu attālinātas izmantošanas par tehniskajiem resursiem atbildīgā persona novērtē izmantošanas riskus un veic nepieciešamos pasākumus (nosaka aizsardzības līdzekļus) risku mazināšanai un nodrošina, ka izmantojot iekārtas, kas atrodas ārpus iestādes telpām, vai kas neatrodas iestādes valdījumā, būtu iespējams piekļūt sistēmai ar sistēmas administratora kontu, tikai izmantojot daudzfaktoru autentifikāciju.
28. Par tehniskajiem resursiem atbildīgā persona ne retāk kā reizi gadā veic IS drošības risku analīzi saskaņā ar Pārziņa noteikumiem “Informācijas sistēmu drošības iekšējie noteikumi” un “Informācijas sistēmu drošības riska pārvaldības plāns”.
29. Pārzinis nosaka IS fiziskās drošības prasības, lai aizsargātu darbiniekus, informācijas resursus, tehniskos resursus, piekritīgas telpas un infrastruktūru no destruktīvas ietekmes, ko var izraisīt cilvēku tīša, netīša rīcība vai bezdarbība, tehniskas norises vai dabas faktori.
30. Telpas, kurās izvietoti IS tehniskie vai informācijas resursi vai, ko izmanto informācijas aprites procesā, grupē pa drošības zonām. Drošības zonu dalījumu un skaitu nosaka, vadoties no tajās esošo tehnisko un informācijas resursu vai to daļu klasifikācijas kategorijas, kā arī telpu funkcionālā pielietojuma:
    1. publiskā zona ir pieejama visiem darbiniekiem un apmeklētājiem, tiek veikta novērošana;
    2. ierobežotas pieejamības zona ir pieejama tikai tiem darbiniekiem, kuriem darba pienākumu izpildei tas nepieciešams, bet apmeklētājiem – tikai darbinieku pavadībā.
31. Pārzinis nodrošina IS tehnisko resursu ekspluatācijas apstākļu atbilstību ražotāju noteiktajām ekspluatācijas un uzglabāšanas normām.
32. Šajos noteikumos noteiktās ikdienas procedūras aizstāj ar krīzes pārvaldības procedūrām, ja IS darbības atjaunošanas laiks pārsniedz pieļaujamo, kā arī, ja IS konstatēts datu zudums.

VII. Noslēguma jautājumi

1. Šos noteikumus pārskata vismaz reizi gadā, kā arī:
   1. ja izmaiņas IS var ietekmēt IS drošību;
   2. ja mainījušies vai atklāti jauni IS drošības apdraudējumi;
   3. ja pieaug IS drošības incidentu skaits vai noticis nozīmīgs incidents.
2. Ar šo noteikumu parakstīšanu spēku zaudē Carnikavas novada domes 2018. gada 25. aprīļa noteikumi Nr. INA/2018/14 “Informācijas sistēmu drošības politika”.

Pašvaldības domes priekšsēdētāja K.Miķelsone

*@ ITN, PSN, IDR*

Pielikums

Ādažu novada pašvaldības

22.03.2023. noteikumiem Nr. XXXX

**ĀDAŽU NOVADA PAŠVALDĪBAS INFORMĀCIJAS SISTĒMU REĢISTRS**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N.p.k. | IS nosaukums | P | I | K | Pieejamības klase | Sistēmas raksturojums | Paaugstinātas drošības sistēma *(atzīmēt ar X)* | Pamata drošības sistēma  *(atzīmēt ar X)* | Nepārtrauktās darbības laiks | Atjaunošanas  laiks |
| *(atzīmēt A, B, C)* | | |
| 1. |  |  |  |  |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |

*P – Pieejamība*

*I – Integritāte*

*K - Konfidencialitāte*